Abstract of the Disclosure

An apparatus and method for implementing a quantum cryptography system encoding bit values on approximations of elementary quantum systems with provable and absolute security against photon number splitting attacks. The emitter encodes the bit values onto pairs of non-orthogonal states belonging to at least two sets, and such that there does not exist a single quantum operation allowing to reduce the overlap of the states in all the sets simultaneously.